Germany seeks expansion of computer spying

By Kim Murphy, Los Angeles Times Staff Writer

October 30, 2007

BERLIN -- The first evidence was the bombs themselves, packed into a pair of suitcases and left on two passenger trains in northwest Germany. Because of a technical flaw, they never exploded, but not for lack of planning. The laptop of one of the suspects in last year's bungled bombings contained plans, sketches and maps -- a virtual road map to an attack that could have killed dozens.

A proposal to secretly scan suspects' hard drives causes unease in a nation with a history of official surveillance.

What if law enforcement agents had been able to secretly scan the contents of the computer before the attempted attack was carried out?

To the unease of many in a country with a history of government spying through the era of the Gestapo and communist rule in East Germany, law enforcement authorities are using the suitcase bomb case to argue for measures that would significantly expand their ability to spy on the once-private realm of My Documents.

Expanded surveillance laws since the Sept. 11 attacks already have enabled many Western governments to monitor telephone and e-mail traffic, the conversation in Islamic militants' chat rooms and the websites visited by terrorism suspects.

Now, along with several other European countries, Germany is seeking authority to plant secret Trojan viruses into the computers of suspects that could scan files, photos, diagrams and voice recordings, record every...
keystroke typed and possibly even turn on webcams and microphones in an attempt to gain knowledge of attacks before they happen.

"What this case showed us is that they are using laptops, they are using computers, and it would have been very, very helpful to track them down with online searches," said Gerhard Schindler, director of the German Interior Ministry's counter-terrorism bureau.

The proposal significantly raises the stakes in the balance between privacy and security here in Germany, where the idea of a watchful government calls up images of agents sitting in basements at old typewriters listening to secret microphones.

Here in Berlin, T-shirts with a photograph of Interior Minister Wolfgang Schaeuble and the logo "Stasi 2.0," a reference to the former German Democratic Republic's infamous secret police, have suddenly become popular. Many fear a return to the 1970s, and the often-severe anti-terrorism measures wielded by then-West Germany to fight the devastating tactics of the leftist Red Army Faction.

And in today's high-tech world, the proposed measure causes a chill to those who see hard drives as the new window to the soul.

"Back in the '80s when people were fighting the census, it was because they feared the state could find out that they were not honest toward the tax authorities or something like that," said Sven Lueders, head of the Humanist Union of Berlin, which helped organize a recent protest against the so-called Bundestrojaner, or federal Trojans. "Now what people fear is that the state can actually look into your computer. Because almost everybody has something on his computer that he doesn't want somebody else to see."

"If you spy on my telephone calls, you can never have as big a picture of me as if you can read my hard drive," said Constanze Kurz, an activist with the Berlin-based hacker organization the Chaos Computer Club, which has pledged to find and publicize the first government Trojan.

"My communications, my private photos, my private films, all of my research. And if you install that Trojan on the computer, you can look not only at this data on the hard drive, but you can see what I'm typing, you can collect my thoughts as I'm typing them in," she said. "If you give me your computer for one hour, I will know everything about you."

Already, Romania, Cyprus, Latvia and Spain have laws that allow "online searches," according to a report from Germany's Interior Ministry, which conducted an informal survey in Europe. Switzerland and Slovenia appear to also allow such searches, and Sweden is in the process of adopting similar legislation, the report said.

In the U.S., where battles are being fought over warrantless surveillance of telephone and Internet communications, the FBI is known to have implanted software designed to identify target computers. But it is unknown, and the FBI won't say, whether the government has tried to surreptitiously search the contents of hard drives.

"I'm not aware of that technique being used in the United States," said Marc Rotenberg, president of the Washington-based Electronic Privacy Information Center. "But it's also not clear, given the current view of the president on his powers to conduct electronic surveillance, that it hasn't been used."

Europe has been scrambling in recent months to adopt new counter-terrorism measures as recent arrests in Britain, Germany and Denmark have shed light on the increased number of militants raised in Europe.

On Nov. 6, the European Union's justice commissioner, Franco Frattini, will propose a new set of counter-terrorism measures that is expected to include proposals to block Internet sites offering bomb-making recipes and
Germany seeks expansion of computer spying - Los Angeles Times

The mood in Germany since the latest wave of arrests in September has been tense, with senior officials warning that they cannot hope to stop all the plots believed to be underway.

"A terrorist attack with nuclear weapons is certain. The question is no longer whether such an attack could be carried out by terrorists, but when," Schaeuble told the Frankfurter Allgemeine newspaper in September.

Defense Minister Franz Josef Jung has warned that he would be prepared to order the shooting down of a commercial airliner hijacked by terrorists under emergency laws, despite a court ruling that held such a measure illegal.

Police say that although the current authority to enter a suspect's home and seize computers and storage drives for inspection is helpful, there are times when the ability to probe without the suspect's knowledge, by way of an e-bug implanted when he unknowingly opened an e-mail attachment, might yield crucial information.

"I can imagine lots of cases where it's sensible not to do a physical search first," said Konrad Freiberg, chairman of Germany's police union, who is an advocate of the proposed new authority.

"For example, if a suspect is under telephone wiretapping and we know from his phone calls that he's planning an attack. At the moment, we would have to go to his apartment and search his apartment. But then he would know that we are there. And maybe in this case, it would be more sensible to let it go for a couple of days, look at what he's doing, see what he's planning, and do that secretly, in hiding," he said.

Federal intelligence agencies already had been conducting these kinds of online searches but were forced to halt the practice in February, when the Federal Court of Justice ruled it was illegal. The interior minister said such searches would not resume before the passage of legislation, and possibly an amendment of Germany's Basic Law, to allow them.

The government is awaiting a decision from the federal Constitutional Court, which is hearing a legal challenge to the procedure brought in a provincial case, and, depending on the outcome, could present proposed legislation by the end of the year.

Critics of the proposed policy complain that it could circumvent the normal, adversarial legal procedures for searches precisely because of its secrecy.

"It is already possible with the decision of a judge to physically search computers, but it has to be approved by a court. And since it is necessary to have it approved by a court, it is also possible to object," said Hans-Christian Stroeble, a member of parliament from the Green Party. "But if you want to do it secretly, it runs completely out of the control of legal procedure.

"What we fear is that without any hint of a criminal background, police can secretly go into computers, maybe even the computers of political opponents, and spy them out, gaining access to personal data like photos, diaries, love letters, things like that," Stroeble said.

Law enforcement authorities emphasize that they are seeking an official legislative sanction to ensure that proper protections are in place.

"We need to put this into a clear framework of rules, which means it has to be clearly defined who is going to allow online searches," Schindler said. "It's not going to be a police officer who decides that; it of course will be a..."
Computer aficionados say it's doubtful that any criminal worth his salt would be foolish enough to open an e-mail attachment with a Trojan virus embedded in it. Government officials responded that they might embed the programs in communications from the tax authorities -- a proposal that raised more controversy, with critics saying it would cause the public to mistrust all government communications.

German authorities are also trying to regulate the distribution of militant material on the Internet. In a groundbreaking case in the city of Celle, an Iraqi Kurdish immigrant identified only as Ibrahim R. is on trial for forwarding videos made by Osama bin Laden and other Al Qaeda leaders, available elsewhere on the Internet, into Islamic militant chat rooms.

Prosecutors, who have charged him with supporting terrorism, say his postings amount to conducting a "virtual jihad."

But Klaus Ruether, his defense lawyer, said anyone might forward such videos; Ibrahim R.'s crime is that he seemed to agree with the points of view expressed, the lawyer said.

"If a person can be punished only because of what they suppose he has in his mind," Ruether said, "then we have crossed an important line."

kim.murphy@latimes.com